Universidad de Buenos Aires

Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática
Trabajo Final

Tema
Gestión de Riesgos en Tiempos de Crisis

Título
Guía para la implementación de la gestión de riesgos a la seguridad de la información en tiempos de crisis

Autor:
Nubia Esperanza Aparicio Joya

Tutor:
Mg. Paula María Angeleri

Año 2012
Cohorte 2011

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente la autora manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e internacional de propiedad Intelectual.

Firmado,
Nubia Esperanza Aparicio Joya
DNI: 94744312
Pasaporte: 632769

RESUMEN

El presente trabajo tiene como finalidad estudiar los diferentes hechos o acontecimientos que se presentan en las crisis, mediante un enfoque analítico, con el fin de evaluar y contrarrestar los riesgos, haciendo foco en la seguridad de la información.

Los aspectos a tener en cuenta dentro del desarrollo del trabajo son:

- Analizar los diferentes eventos y/o acontecimientos que desencadenan las crisis con el fin de acotar puntos clave.
- Analizar las bases teóricas y elementos fundamentales que se plasman en los diferentes escritos de gestión de riesgos en tiempos de crisis.
- Identificar las buenas prácticas que deberían seguirse en el proceso de gestión de seguridad de la información durante los tiempos de crisis.

Se tendrá en cuenta el relevamiento de regulaciones, normas, estándares y mejores prácticas en temas de seguridad de la información y Gestión de Riesgos.

Se utilizarán como herramientas de apoyo a la investigación teórica y metodológica los papers y demás materiales publicados especialmente en la Web, sobre las crisis de los últimos tiempos y la gestión de riesgos en tiempos de Crisis.

Palabras Claves: riesgos, seguridad de la Información, crisis, gestión de riesgos.

Tabla de contenido

Lista de Figuras

Lista de Tablas

INTRODUCCIÓN

El objetivo del presente escrito es realizar una guía de buenas prácticas para gestionar los riesgos en tiempos de crisis dentro del marco de la seguridad de la información.

Dando como alcance la elaboración de cuestionarios que faciliten a la organización a identificar y evitar los aspectos que puedan ser generadores de crisis.

Las organizaciones a menudo encuentran diferentes aspectos generadores de riesgo que aumentan en tiempos de crisis, y que deben ser controlados y evaluados, teniendo en cuenta la seguridad de la información. El presente trabajo aborda esta problemática, a través de 4 capítulos principales. El capítulo 1 proporciona un marco de entrada al tema a desarrollar donde se explican las causas que desencadenan las crisis, dando como ejemplo las crisis financieras de 2008 y 2011 en Estados Unidos y Europa, destacando los aspectos generadores de dichas crisis. En el capítulo 2 se plantea porqué es necesario gestionar los riesgos en tiempo de crisis, adicionalmente se presentan algunos aspectos a tener en cuenta para lograr una adecuada gestión de riesgos, y acciones para administrar el riesgo de manera inteligente. En el capítulo 3 se detallan aspectos de las normas y estándares para la gestión de seguridad de la información, porque inyectar seguridad de la información a la gestión de riesgos. En el capítulo 4 se elabora una guía de las mejores prácticas aplicando seguridad de información a la gestión de riesgos en tiempo de crisis, integrando los primeros tres capítulos, dando un valor agregado a lo investigado. Por último se detallan las conclusiones que surgen de este trabajo.

CAPITULO 1

CONCEPTO DE CRISIS Y SU IMPACTO ORGANIZACIONAL

Como punto inicial se explica qué es una crisis, y por qué se desencadenan estos acontecimientos que tienden a eliminar el punto de equilibrio de las organizaciones y su entorno.

1.1. ¿Por Qué Se Desencadenan Las Crisis?

Las crisis son fenómenos o hechos inesperados que ocurren de manera eventual, generando caos y confusión a las naciones, gobiernos, empresas y la sociedad en general.

Las crisis en las empresas se desencadenan por diferentes aspectos, causas internas y causas externas que de alguna manera no se tuvieron en cuenta o no se profundizó en ellas, ya sea por desconocimiento del entorno y del ambiente organizacional, o por que dichos aspectos no parecieron importantes o prioritarios para el desarrollo de su objetivo.

El caos se genera cuando las empresas no se encuentran preparadas para enfrentar las crisis o no tuvieron en cuenta aspectos importantes que les pudieran afectar. Los acontecimientos del entorno cuando se presentan los momentos críticos, hacen que las empresas duden de sus capacidades, los empleados se asusten o simplemente sientan miedo, especialmente porque no saben que pueda llegar a pasar en caso que la empresa no puede superar este momento de crisis. Estas actitudes hacen que se generen diferentes hechos para que las organizaciones reevalúen sus planes de acción, quieran replantear la estrategia organizacional, a nivel económico y financiero, considerando aspectos que le brinden seguridad, solidez y confianza a sus clientes internos (socios, accionistas, directivos y empleados) y clientes externos (proveedores, distribuidores, compradores).

Oriol Amat explica que las consecuencias de una importante crisis para muchos directivos, es buscar las razones de sus problemas en causas de tipo externo, aunque hay que analizar más las causas internas, aquellas que están en el ámbito de actuación de la propia empresa.[1]

Para entender un poco más los aspectos que se presentan en momentos difíciles y que pueden ser generadores de crisis dentro de una empresa, se explicaran los más relevantes:

1.1.1. Problemas en las personas [1]: El recurso humano presenta una serie de comportamientos que puede afectar los objetivos y estrategias organizacionales como se expone a continuación:

¿Quién? [1]

- Falta de Iniciativa y diligencia para afrontar, intervenir y accionar en las situaciones difíciles.
- Falta de visión de negocio a mediano y largo plazo.
- Conflictos entre accionistas, directivos y líderes de grupos, desacuerdos interpersonales e interdepartamentales.
- Falta de compromiso, motivación y sentido de pertenencia del personal (liderazgo deficiente, selección de empleados poco asertiva, capacitación y formación insuficiente, políticas de incentivos poco atractivas).
- Falta de clima laboral optimo, comunicación no efectiva (arrogancia y superioridad).
- Conflictos laborales constantes, incremento de las tensiones laborales, alta rotación del personal, renuncia de ejecutivos.
- Incremento en la tensión laboral, altos niveles de estrés.
- Falta de manejo y optimización del factor tiempo.
- Falta de calidad en el trabajo y mejor calidad de vida.

Las personas son determinantes para que las empresas puedan salir de las crisis; tienen efectos positivos y negativos, su contribución se da:

- De manera Positiva; aportando ideas innovadoras, progresistas y retadoras, permitiendo a la organización proyectarse con agilidad y visión estratégica.
- De manera negativa; pueden llevar a la empresa a la quiebra o cierre de la misma, por manipulación inadecuada de las herramientas, programas y procesos y tecnologías.

1.1.2. Problemas referidos a la planificación estratégica [1]: El entorno es uno de los aspectos que debe tener en cuenta la organización para desarrollar sus estrategias ya que se puede ver afectada en cuanto a:

¿Qué hace la empresa frente al entorno competitivo? [1]

- Sector empresarial con inconvenientes (perspectivas negativas del entorno)
- Desconocimiento de la competencia y de las estrategias de mercado que manejan.
- Innovación tecnológica y de gestión insuficientes (falta de flexibilidad).
- Productos y procesos obsoletos.
- Planes estratégicos no concretos, inviables, irrealizables o mal planteados (Gestión Administrativa, análisis DOFA, plan de TI, plan de SI, control de riesgos)
- Exceso de diversificación.
- Fracasos continuos en el lanzamiento de nuevos productos y /o servicios.
- Desconocimiento de los nichos de mercado y mercados objetivos (perfil de cliente)
- Infraestructura y equipos obsoletos
- Imagen corporativa decadente o decreciente.
- Objetivos poco vanguardistas y retadores.

La administración estratégica invita a conocer el entorno y crear acciones vanguardistas y retadoras que permitan a una organización ver sus falencias y sus fortalezas, a fin de buscar oportunidades de crecimiento y mejora continua reconociendo sus debilidades y trabajando en ellas para llegar a la excelencia.

Si se tienen los planes definidos para lograr cumplir los objetivos y existen procesos y procedimientos claros, desarrollados con calidad y eficiencia, esto permitirá que se cumplan las metas trazadas por la organización, por eso es importante que la institución no deje de lado sus planes estratégicos aun en tiempos de crisis.

1.1.3. Problemas operativos[1]: Los aspectos operativos relacionados con los procesos, los clientes y las finanzas, son factores que no dan espera y deben ser controlados en la organización, a continuación se presentan algunos aspectos importantes:

¿Cómo lo hace la empresa?[1]

Procesos:

- Costos excesivos (precios de compra elevados, ineficiencia en la gestión de activos).
- Problemas de calidad: errores, devoluciones, quejas de clientes
- Deficiente servicio post-venta.
- Lentitud en los procesos de toma de decisiones

Clientes:

- Ingresos insuficientes (políticas de *marketing poco acertados*, precios de venta inadecuados, publicidad deficiente.
- Clientes insatisfechos
- Falta de fidelización de clientes.

Administración y Finanzas:

- Endeudamiento Excesivo y liquidez insuficiente (nulidad en inyección de capital por parte de los socios, exceso de inversiones, mala distribución de las ganancias, reparto excesivo de dividendos a los accionistas).
- Descontrol: falta de planeación estratégica, de gestión, falta de control de riesgos, de seguridad.
- No comunicación asertiva, oportuna y efectiva (falta de información, mala gestión de riesgos, diseño organizativo defectuoso).
- Pérdidas (por los ingresos insuficientes y los costos excesivos, aumento de los costos y gastos de operación y distribución, aumento de devoluciones, quejas y reclamos, problemas de inventarios: pérdidas y robos).

La gestión operativa es importante porque los procesos deficientes pueden desvirtuar muchos detalles claves para el éxito dentro de la organización y en determinado momento generar crisis.

Una vez razonados los aspectos organizacionales mencionados anteriormente, se hace necesario analizar los hechos que ocasionaron las crisis financieras de los años 2008 y 2011 en Estados Unidos y Europa; para entender como impactaron a empresas, no necesariamente por no tener identificados o controlados los riesgos del entorno dentro de las compañías, sino como acontecimientos que se fueron masificando en el tiempo,

convirtiéndose en una bola de nieve que arrasó con sectores económicos completos, afectando la economía de los países.

1.2. Crisis Financieras de 2008 y 2011:

La crisis financiera mundial del 2008 se presentó debido a que las entidades financieras comenzaron a dar créditos a personas con capacidad crediticia baja y a respaldar dichos créditos en activos intangibles denominados bonos y acciones para cubrir dichas deudas lo que generó un desequilibrio financiero mundial.

Algunas de las causas que originaron dicho desequilibrio fue por la estrecha relación existente entre los mercados globales, lo que implicó que al desencadenarse una crisis en algún lugar del mundo generará una influencia inmediata en la economía de cualquier país, creando preocupación, incertidumbre y desconcierto en todos los ámbitos relacionados al mundo financiero y económico.

Como lo menciona Isaías Covarrubias [2]: "La situación se revirtió en el 2008, cuando el precio de las viviendas comenzó a caer abruptamente y surgieron los problemas masivos de impago de las hipotecas, especialmente en Estados Unidos, epicentro de la crisis. En el invierno de 2008-2009 el estallido de la burbuja financiera se había convertido en una crisis de consecuencias impredecibles. La bolsa de valores se desplomó, los créditos se congelaron, algunos bancos quebraron mientras los más grandes fueron rescatados mediante financiamiento gubernamental. Los problemas financieros en los Estados Unidos no tardaron en alcanzar a Europa. En los momentos más álgidos de la crisis, la economía norteamericana perdía alrededor de 700.000 empleos cada mes y el comercio mundial se restringía a tasa más rápidas que durante la Gran Depresión en 1930. No obstante, hacia el verano del 2009 la economía mundial mostraba signos de una leve recuperación, lo cual continuó durante el 2010.

La interdependencia existente entre los mercados bursátiles globales generó una caída en el apalancamiento financiero y del gasto, creando un impacto negativo en el racionamiento del crédito y de la liquidez. Lo cual se viene afectando con la globalización de la economía y las actividades de mercados de capitales".

Las crisis financieras y la recesión económica que las precede son las que han afectado en forma significativa la historia de la humanidad, países, gobiernos, sectores económicos y en especial de las organizaciones, por que afectan la economía en general, viéndose obligados a reorientar las

estrategias empresariales, tener otra visión de negocio y ver de manera objetiva otros aspectos que antes no se tenían en cuenta.

A continuación se analizan algunos aspectos de importancia para el sector empresarial y que han sido generadores de crisis.

1.3. Aspectos A Tener En Cuenta Para Enfrentar Las Crisis:

Entender el comienzo y el final de una crisis no es fácil pero cuando una organización tiene definidos sus objetivos estratégicamente y conoce el entorno en el que se desenvuelve, le es más fácil identificar los riesgos que en determinado momento pueden llegar a afectarla. Cuando se está atento a las diferentes señales del entorno, se pueden identificar y preveer circunstancia que puedan ocasionar que la economía empresarial decline o que su actividad se vea afectada.

Aunque las empresas se preparan para enfrentar momentos de dificultad, realizando gestión de riesgos, mediciones de las amenazas y debilidades, no son lo suficientemente completas para determinar todos los fuentes posibles de riesgos, a fin de analizar cuales se requiere mitigar, incluso a veces no son adecuadas para reconocer si se está o no frente a un riesgo, debido a que los aspectos del entorno varían cuando llegan las crisis.

Más aun los indicadores se ven alterados y se presentan poco asertivos en su aplicabilidad; dejan de ser una opción de respuesta y optimización para que las organizaciones no se vean tan impactadas; por el contrario dichos indicadores en momentos de dificultad ocasionan tensión, adversidad, descontento y frustración, debido a que no se obtienen los resultados esperados.

En razón de lo anterior es necesario identificar el hecho que género la crisis, los aspectos relevantes que fueron alterados en el entorno y los que pueden representar peligro al interior de la organización; se deben conocer las fortalezas y tener la habilidad para reconocer las debilidades y las

amenazas creando oportunidades y ventajas competitivas favorables para explotar por parte de la empresa.

Ante la presión externa el individuo tiende a centrar su atención en lo urgente, dejando de lado lo importante, por esta razón natural es común que los directivos y gerentes cambien la prioridad de las actividades a realizar, pudiendo ser esto contraproducente para la organización.

Por esta razón se considera que es imprescindible gestionar los riesgos, aun en tiempo de crisis, y que es necesario proporcionar una guía que facilite a los directivos y gerentes mantener este proceso de manera eficaz en los tiempos en que enfrenten más presiones, los capítulos siguientes cumplen este objetivo.

CAPITULO 2
PROCESO DE GESTIÓN DE RIESGOS

En este capítulo se explica el proceso de gestión de riesgos y su contribución en tiempos de crisis, a fin de evaluar los aspectos organizacionales que se impactan.

2.1. Proceso Gestión de Riesgos Según IRAM 17550 [11]:

La gestión de riesgos es una parte integrante del proceso de gestión. Gestión de riesgos es un proceso multifacético, por lo que las tareas involucradas son a menudo llevadas a cabo por un equipo multidisciplinario. Es un proceso iterativo de mejora continua, cuya incorporación en las prácticas o procesos de negocio existentes resulta beneficiosa.

Los elementos principales del proceso de gestión de riesgos son los siguientes:

- **Establecer el contexto:** Establecer los contextos estratégico, organizacional y de gestión de riesgos en los cuales tendrá lugar el resto de los procesos. Deberán establecerse los criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.

- **Identificar riesgos:** Identificar qué, por qué, dónde, cuándo y cómo los eventos podrían impedir, degradar, demorar o mejorar el logro de los objetivos estratégicos y de negocio de la organización.

- **Analizar riesgos:** Determinar los controles existentes y analizar los riesgos en términos de consecuencia y probabilidad en el contexto de tales controles. El análisis debería considerar el rango de consecuencias potenciales y cuan probable es que esas consecuencias puedan ocurrir. Consecuencia y probabilidad deberían ser combinadas para producir un nivel estimado de riesgo.

- **Evaluar riesgos:** Comparar los niveles estimados de riesgo contra los criterios preestablecidos y considerar el balance entre beneficios potenciales y resultados adversos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de gestión. Si los niveles de riesgo establecidos son bajos podría caer en una categoría aceptable y no se requeriría tratamiento.

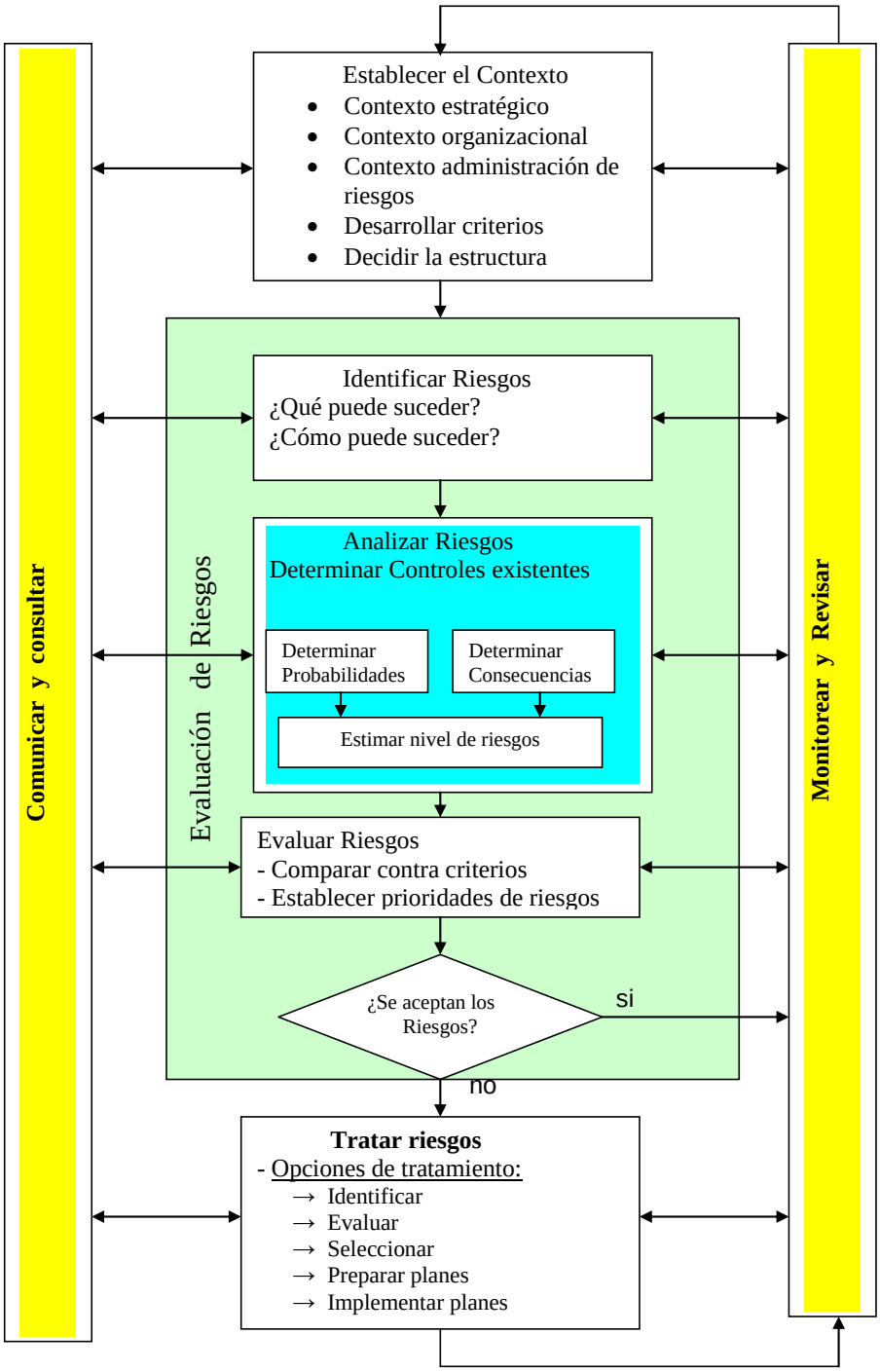
- **Tratar riesgos:** Si los niveles de riesgo establecidos son bajos y son tolerables entonces no se requiere tratamiento. Para otros riesgos desarrollar e implementar estrategias y planes de acción específicos costo-beneficios para aumentar los beneficios potenciales y reducir los costos potenciales.

- **Monitorear y revisar:** Monitorear y revisar el desempeño del sistema de gestión de riesgos y procurar detectar cambios que pudieran afectar la adecuación o beneficio de costo de los controles.

- **Comunicar y consultar:** Comunicar y consultar con interesados internos y externos según resulte apropiado en cada etapa del proceso de administración de riesgos e interpretando al proceso como un todo.

La gestión de riesgos es un proceso iterativo que puede contribuir a la mejora organizacional. Puede ser aplicada a todos los niveles en una organización: a nivel estratégico y a niveles tácticos y operacionales. También puede ser aplicada a proyectos específicos, para sustentar decisiones específicas o para administrar áreas específicas de riesgo reconocidas. Para cada etapa del proceso deberían mantenerse registros adecuados, suficientes como para satisfacer a una auditoría independiente.

Figura 1. Proceso de Gestión de Riesgos



Fuente: Norma IRAM 17550

2.2. Por qué Gestionar los Riesgos?

El sistema empresarial tiene un amplio historial de crisis financieras que debieron haberse podido evitar, abriendo todo tipo de discusiones sobre los riesgos que afectan a las organizaciones y que toman un lugar preponderante en tiempos de crisis.

Como indica Oriol Amat en la actualidad, el sistema financiero global está enfrentando una crisis histórica tanto crediticia como de liquidez, lo que ha quedado en evidencia ha sido la incapacidad de la alta dirección en implementar una gestión de riesgos que estuviera acorde con la creciente innovación y complejidad de los mercados financieros. La falta de una adecuada gestión de riesgos operacionales provocó los grandes colapsos de empresas de renombre mundial [1].

En momentos de dificultad es necesario realizar gestión de riesgos de manera objetiva, autocrítica y vanguardista, como primera medida se deben identificar las amenazas: realizar una lista de los aspectos que pueden llegar a afectar a la organización, identificar aquellos que pueden tener un alto impacto y priorizar soluciones. Hay que actuar de manera ágil, eficaz y eficiente, tener en cuenta los detalles y buscar alternativas innovadoras que se puedan convertir en oportunidades para el negocio.

Lo anterior implicar realizar gestión de riesgos como una herramienta “preventiva” no como herramienta "defensiva"; la diferencia consiste en tener claros cuales son los aspectos que afectan la empresa. Si se tiene el análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) implementado y actualizado para los ámbitos de la organización, esto actuaria como una herramienta preventiva la cual ayudará al nivel ejecutivo a tomar decisiones, acciones inmediatas y favorables para la empresa.

Figura 2. Ciclo de mejora continua de la gestión de riesgo

Fuente: Elaborada utilizando como referencia Tabla ISO/IEC 27005 página 6

La figura anterior muestra el ciclo de gestión de riesgo donde se debe mantener una retroalimentación constante llegando a la mejora continua, previniendo los sucesos “imprevistos” y su impacto en la organización.

Dentro del análisis de riesgos se deben tener en cuenta el riesgo residual y riesgo total así como también el tratamiento del riesgo, evaluación del riesgo y gestión del riesgo entre otras.

Una vez realizado el análisis de riesgos hay que realizar controles y seguimiento respecto a los riesgos residuales que se identifiquen: [3]

Riesgo Residual:

Acciones y actividades [3]

- Controlar el riesgo.- Fortalecer los controles existentes y/o agregar nuevos controles.
- Eliminar el riesgo.- Eliminar el activo relacionado y con ello se elimina el riesgo.
- Reducir el riesgo: crear mecanismos que permitan reducir el riesgo cuando este no se puede eliminar.
- Compartir el riesgo.- Mediante acuerdos contractuales parte del riesgo se traspasa a un tercero.
- Aceptar el riesgo.- Se determina que el nivel de exposición es adecuado y por lo tanto se acepta.

Se deben crear políticas de administración del riesgo implementando un proceso continuo donde se evalúe periódicamente las vulnerabilidades encontradas analizando su afectación, realizando cálculos de probabilidad y ocurrencia dentro de las diferentes etapas del riesgo, como una mecánica de retroalimentación dentro de un esfuerzo del día a día a fin de medir el impacto futuro en la estructura de riesgo de la organización.[3]

2.3. Aspectos Claves Para Una Adecuada Gestión De Riesgos:

En función de la bibliografía relevada, y de la experiencia profesional surgen ciertas prácticas que se aconseja seguir, para minimizar los riesgos a los que una organización está expuesta:

- Utilice herramientas de apoyo**,** existen herramientas de evaluación de riesgos en el mercado en las que se puede apoyar la empresa.[3]
- Conozca y emplee las regulaciones y normas que tratan el riesgo para el beneficio de la organización; algunas de esas normas son[3]:

  - "Comunicación "A" 4609 del BCRA para entidades Financieras • Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.
  - ISO/IEC 27001 • Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)
  - ISO/IEC 27005 • Esta Norma proporciona directrices para la Gestión del riesgo de Seguridad de la Información en una Organización. Sin embargo, esta Norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.
  - Basilea II • Estándar internacional que sirve de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.
  - Ley Sarbanes Oxley (SOX) • Impulsada por el gobierno norteamericano como respuesta a los mega fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros".[3]

- Cree indicadores de gestión y medición en todos los departamentos de la empresa, a nivel de procesos y resultados realice estadísticas de aciertos y errores, evalúe la causa y efecto que ocasionan inconvenientes y cree acciones para evitar que vuelvan a ocurrir. Desarrolle controles e

impleméntelos en conjunto formando una arquitectura de seguridad con la finalidad de preservar las propiedades de confidencialidad, integridad y disponibilidad de los recursos objetos de riesgo con la finalidad de que estos sean efectivos.

- Capacite y entrene constantemente el personal para que estén preparados para una eventualidad, creando sus propios indicadores y mediciones de resultados y de inconvenientes presentados, analice las brechas y los puntos ciegos, cree estándares de seguridad física y lógica realice control de riesgos.
- Cree escenarios de conflicto e involucre al personal busque mediante la participación desarrollar habilidades para contrarrestar los riesgos y crear políticas de anti-crisis.
- Cree dentro del proceso de análisis de riesgo la matriz de riesgo, en este documento se plasman los elementos identificados, relacionando los cálculos realizados, análisis necesarios para lograr una correcta administración del riesgo, haciendo referencia a la gestión de los recursos de la organización.

2.4. Acciones Para Administración De Riesgo Inteligente:

Pasos para lograr una gestión de Riesgo Inteligente según Deloitte[5]:

- "Amplíe su visión del riesgo. No limite sus deliberaciones a la prevención de fraudes, protección de inventarios, seguridad de TI, todos son importantes, pero tienen más relación con "sobrevivir" que con el "tener éxito". Adopte el concepto de Riesgo Inteligente para lograr un equilibrio adecuado entre la protección de valor y la creación de valor.[5]

- Examine detalladamente al Consejo de Administración. Evalúe la estructura de gobierno corporativo del riesgo en el Consejo de Administración y en sus comités. Determine hasta qué punto se supervisa el riesgo. Valore si el enfoque del Consejo de Administración es práctico y sensible a los retos. Para su evaluación, incluya el apoyo de auditoría interna o de un tercero externo. [5]

- No subestime al reto. El trabajo de un Consejo de Administración no empieza y termina con el informe sobre el riesgo. Más bien requiere un compromiso de tiempo e intelecto para entender los problemas y las actividades subyacentes al informe. el Consejo de Administración debe participar en un diálogo significativo en relación con subestimar o sobreestimar el riesgo es decir, considerar si la empresa es demasiado renuente al riesgo y, al mismo tiempo, determinar si tiene la suficiente cobertura en las áreas expuestas al riesgo. [5]

- Piense en un esquema de riesgo. No aborde el riesgo de manera improvisada. Asegúrese de que exista un esquema apropiado que respalde las actividades de gobierno corporativo del riesgo. [5]

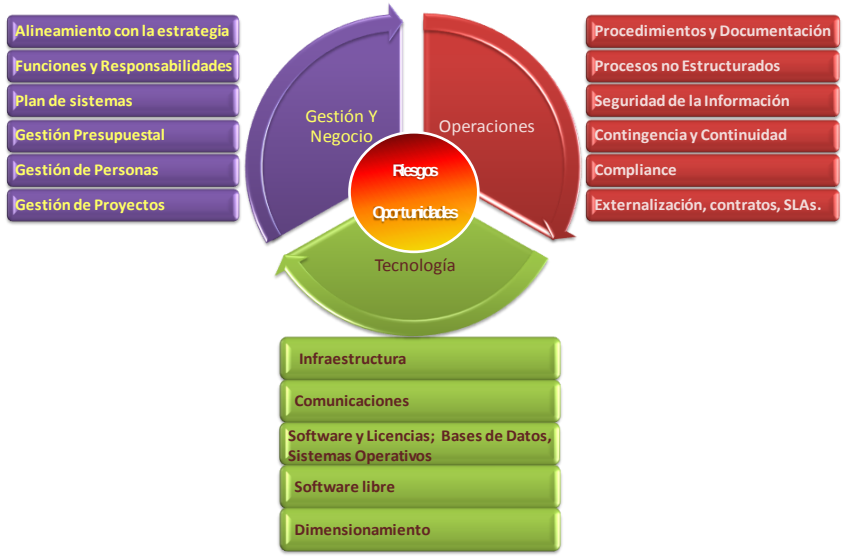
- Alinéese con la dirección. Trabaje en armonía. Asegúrese de que la dirección esté alineada y coordinada con el punto de vista sobre el riesgo que tiene el Consejo de Administración. [5]

- Solicite a la dirección los preparativos necesarios para que el consejo de administración consiga el nivel más alto y más práctico posible de gobierno corporativo de riesgo. [5]

- Evalúe el desempeño del riesgo. Asegúrese de establecer evaluaciones periódicas e independientes para estimar la eficiencia de todo el programa de administración del riesgo. El Consejo de Administración debe determinar si los procesos de riesgo son lo suficientemente rigurosos. [5]"

El gráfico que se observa a continuación integra los aspectos de gestión de riesgos, operaciones y tecnología a tener en cuenta en la administración del riesgo y como ellos están constantemente interactuando, por ende su control debe ser continuo acorde con la infraestructura empresarial.

Figura 3. Diagnosis de riesgos y oportunidades derivados de los SI/TI en la empresa



Fuente: http://blog.tataki.es/servicios/soporte-direccion-si-ti/

CAPITULO 3
APLICANDO SEGURIDAD DE LA INFORMACIÓN EN LA ORGANIZACIÓN

3.1. Estándares y Normativas de Seguridad:

Como lo indica el documento “Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa” [6], existen organismos que han definido estándares y normas a tener en cuenta para el cumplimiento de la seguridad de la información los cuales se definen a continuación:

- COBIT está basado en marcos de referencia establecidos, tales como CMM de SEI (Software Engineering Institute), ISO 9000, ITIL e ISO/IEC 27002; sin embargo, COBIT no incluye tareas y pasos de procesos porque, aunque está orientado a procesos de TI, es un marco de referencia para gestión y control antes que un marco de referencia para procesos. COBIT se focaliza en lo que una empresa necesita hacer, no cómo lo tiene que hacer, y la audiencia objetivo es la alta gerencia, los gerentes funcionales, los gerentes de TI y los auditores.[6]

- ITIL está basado en la definición de procesos de mejores prácticas para la gestión y el soporte de servicios de TI, antes que en la definición de un marco de control de amplio alcance. Se focaliza en el método y define un grupo más compacto de procesos. Existe material adicional en ITIL v3 que proporciona un contexto estratégico y de negocios para la toma de decisiones de TI, y empieza describiendo el mejoramiento continuo del servicio como una actividad integral, promoviendo el mantenimiento de la entrega de valor a los clientes.[6]

- ISO/IEC 20000, Estándar cuyo objetivo es certificar el sistema de gestión de TI de una empresa, que incluya políticas y un marco de trabajo orientado a procesos, para hacer posible una efectiva gestión e implementación de todos los servicios de tecnología de la información. Se basa en el ciclo PDCA de mejora continua y las mejores prácticas de ITIL. En el apartado “6.6 Gestión de la Seguridad de la Información”. Define como objetivo, gestionar la seguridad de la información de manera eficaz para todas las actividades del servicio. [3]

NOTA. Los términos utilizados por el autor no son los más acertados, ISO/IEC 20000 es una serie de normas que tiene por objetivo el definir los requisitos de un Sistema de Gestión de Servicios, y los lineamientos para implementarlo, mantenerlo y mejorarlo en el tiempo.

- ISO/IEC 27000, Estándar normativo, cuyo objetivo es certificar el SGSI (Sistema de Gestión de la Seguridad de la Información) de una empresa, especificando los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales. [3]

NOTA. Los términos utilizados por el autor no son los mas acertados, ISO/IEC 27000 es una serie de normas que tiene por objetivo el definir los requisitos de un Sistema de Gestión de Seguridad de la Información, y los lineamientos para implementarlo, mantenerlo y mejorarlo en el tiempo.

- ISO/IEC 27001, Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) [3]

- El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para el documento de mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.[6]

Se deben implementar políticas y procedimientos de gestión, que ayuden a que se incorporen normas de seguridad y mejores prácticas dentro de las actividades diarias de la organización. Dichas prácticas deben ser compatibles con un marco de gestión de riesgos y de control apropiados para la organización, para que al ser integrados de manera eficaz con otros métodos y prácticas que se utilicen actualmente, puedan evitar reprocesos innecesarios; llegando a ser eficientes si se mantienen actualizados. Para lograr esto es necesario que la administración y el personal entiendan qué hacer, cómo hacerlo y por qué es importante.

3.2 Importancia De La Aplicación De Estándares:

Todas las empresas necesitan adaptar el uso de estándares y prácticas, para ajustar sus requisitos individuales: [6]

Para apoyar la gobernabilidad [6]

- Proporcionar una política de gestión y un marco de control.
- Facilitar el proceso de asignación de propietarios, responsabilidades para las actividades de SI/TI.
- Alinear los objetivos de SI/TI con los objetivos del negocio, definiendo prioridades y la asignación de recursos.
- Asegurar el retorno de la inversión y optimizar los costos.
- Asegurar la identificación de los riesgos significativos, asignación de responsabilidad en la gestión del riesgo y asegurando a la dirección que se han implementado controles eficaces.
- Organización eficiente de los recursos y existencia suficiente de capacidad (infraestructura técnica, procesos y habilidades) para ejecutar la estrategia de SI/TI.
- Asegurar que las actividades críticas de SI/TI pueden ser monitoreadas y medidas, identificando los problemas y adoptando medidas correctivas.

Para definir los requisitos del servicio, tanto internamente como con los proveedores de servicios [6]

- Estableciendo objetivos claros de SI/TI relacionados al negocio así como métricas.
- Definiendo los servicios y proyectos en términos de usuario final.
- Elaborando acuerdos de niveles de servicio y contratos que pueden ser monitoreados por los clientes.
- Asegurando que los requisitos del cliente han sido plasmados apropiadamente en requisitos operativos y técnicos de SI/TI.
- Considerando los portafolios de servicios y de proyectos en conjunto, a fin de establecer las prioridades relativas, de modo que los recursos se asignen de manera equitativa y viable.

Para verificar la capacidad profesional & demostrar competencia mercado [6]

- Las evaluaciones y las auditorías independientes de terceros.
- Compromisos contractuales.
- Constancias y certificaciones.

Para facilitar la mejora continua[6]

- Evaluaciones de madurez.
- Análisis de brechas.
- Benchmarking.
- Planificación de la mejora.
- Evitar la reinvención de buenos enfoques ya probados.

Como marco para la auditoría, evaluación y una visión externa [6]

- Criterios objetivos y mutuamente entendidos.
- Benchmarking para justificar las debilidades y brechas en los controles.
- Incrementando la profundidad y el valor de las recomendaciones mediante enfoques generalmente aceptados.

Priorización dónde y cómo utilizar estándares y mejores prácticas[6]

- Asegurarse que SI/TI está en la agenda.
- Cuestionar las actividades de gestión en materia de SI/TI para asegurar que los problemas de SI/TI son revelados.
- Guiar a la administración ayudando a alinear las iniciativas de SI/TI con las necesidades reales del negocio. Asegurar que la administración valora el impacto potencial de los riesgos de SI/TI en el negocio.
- Insistir en que el desempeño de SI/TI sea medido y se comunique a la Alta Dirección.
- Establecer un comité de dirección de SI/TI o consejo de gobierno de SI/TI con la responsabilidad de comunicar los aspectos de SI/TI a la Alta Dirección y la administración.
- Insistir en que exista un marco de gestión para el gobierno de TI basada en un enfoque común (por ejemplo, COBIT) y un marco de mejores prácticas para la gestión de servicios SI/TI y seguridad basadas en un estándar global y de facto.

Planificación dónde empezar y asegurar que el proceso de implementación pasos, basados en la guía SI*/TI Governance Implementation Guide* del ITGI[6]

- Establecer un marco organizacional, con objetivos y responsabilidades claras, la participación de todas las partes involucradas.
- Alinear la estrategia de SI/TI con los objetivos del negocio. ¿En cuáles de los objetivos de negocio actuales, SI/TI tiene una contribución significativa? Obtener una buena comprensión del entorno empresarial, el apetito de riesgo, la estrategia del negocio, y su relación con SI/TI.
- Entender y definir los riesgos. Dados los objetivos de negocio, ¿cuáles son los riesgos relativos a la capacidad de SI/TI para cumplirlos? Considerar:
- Antecedentes y patrones de desempeño, factores organizacionales actuales de SI/TI, La complejidad y el tamaño/alcance de la infraestructura de SI/TI existente o prevista, las vulnerabilidades inherentes de la infraestructura de SI/TI existente o prevista, la naturaleza de las iniciativas de SI/TI que están siendo consideradas.
- Definir las áreas objetivo y determinar las áreas de proceso de SI/TI que son críticos para la entrega de valor y gestionar estas áreas de riesgo. (Estratégico, programa, proyecto u operativo).
- Analizar la capacidad vigente e identificar las brechas. Realizar una evaluación de la capacidad de madurez para saber dónde es que más se necesitan mejoras.
- Desarrollar estrategias de mejora y decidir cuáles son los proyectos de mayor prioridad que ayudarán a mejorar la gestión y el gobierno de las áreas importantes como una iniciativa de mejora continua.
- Medir los resultados, estableciendo un mecanismo de puntuación para medir el desempeño actual y monitorear los resultados de nuevas mejoras.

Evitar obstáculo[6]

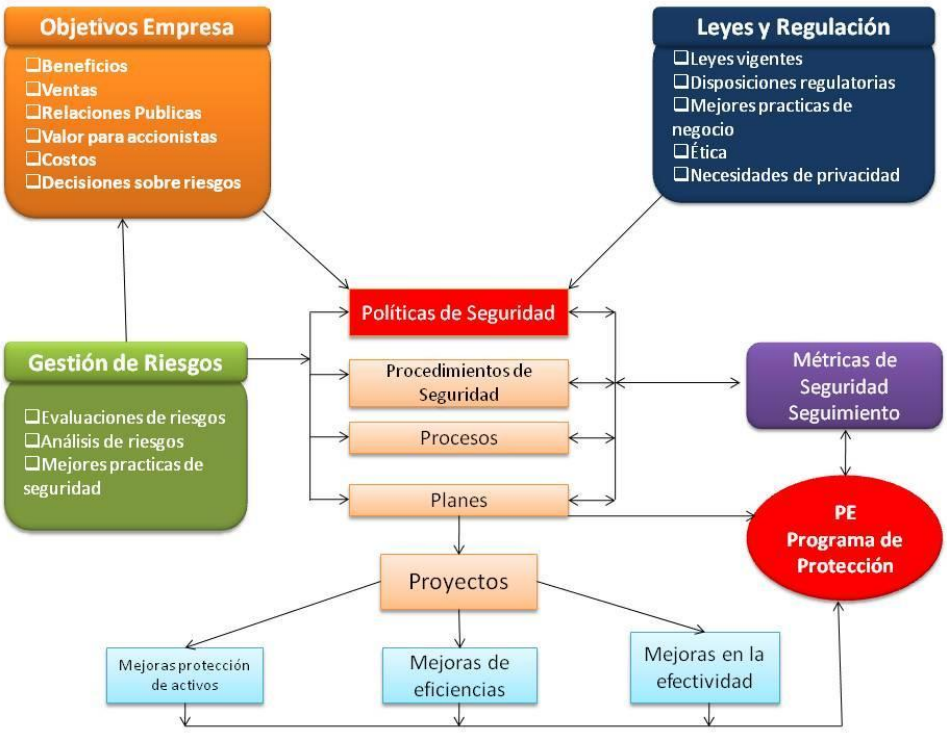
- Tratar la iniciativa de implementación como una actividad de proyecto con una serie de fases en lugar de un solo esfuerzo extraordinario.
- Recuerde que la implementación supone un cambio cultural, así como nuevos procesos. Por lo tanto, un factor clave de éxito es facilitar y motivar estos cambios.
- Asegúrese de que haya una comprensión clara de los objetivos.
- Manejar las expectativas. En la mayoría de las empresas, lograr la supervisión exitosa de SI/TI toma tiempo y es un proceso de mejora continua.
- Concéntrese primero en las áreas donde es más fácil hacer cambios y lograr mejoras, y desde allí, construir paso a paso.
- Obtener el respaldo de la Alta Dirección. Esto necesita estar basado en los principios de la mejor gestión de las inversiones de SI/TI.
- Evitar las iniciativas que se perciben como un ejercicio puramente burocrático.
- Evitar listas de verificación fuera de foco.

3.3 Por Qué La Gestión De Riesgos Contribuye A La Seguridad De La Información:

Como indica la norma ISO/IEC 27001:2005:

"La seguridad de la información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños a las organizaciones y maximizar el retorno de las inversiones y las oportunidades de negocio, en busca de lograr el mayor beneficio con el menor costo.
La seguridad de la información se consigue implantando un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software. Estos controles deberían ser establecidos, implementados, supervisados, revisados y mejorados cuando sea necesario para asegurar que se cumplen los objetivos específicos de seguridad de la organización. Esto debería hacerse en forma conjunta con otros procesos de la administración del negocio". [4 iso-27001-2005-espanol]

Figura 4. Proceso de Gestión de Seguridad de la información



Fuente: seguridad y seguridad.blogspot.com.ar /2009/01/ plan-estrategico-seguridad-powerpoint_18.html . [4]

La figura anterior representa el proceso a realizar una vez definida la política de seguridad alineada con los objetivos de la empresa, marco legal, gestión de Riesgos, métricas de seguridad como un proceso cíclico que se debe estar actualizando y mejorando.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

En cuanto a la gestión de riesgos el ISO/IEC 27001:2005, incluye los siguientes aspectos: [3]

Análisis y Evaluación de Riesgos:

Acciones y actividades[3]

- Identificación de los activos
- Identificación de los requisitos legales y de negocios que son relevantes para la identificación de los activos.
- Valoración de los activos identificados: requisitos legales confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades importantes para los activos identificados.
- Cálculo y evaluación del riesgo, de las amenazas y las vulnerabilidades a ocurrir.
- Evaluación de los riesgos frente a una escala de riesgos preestablecidos.

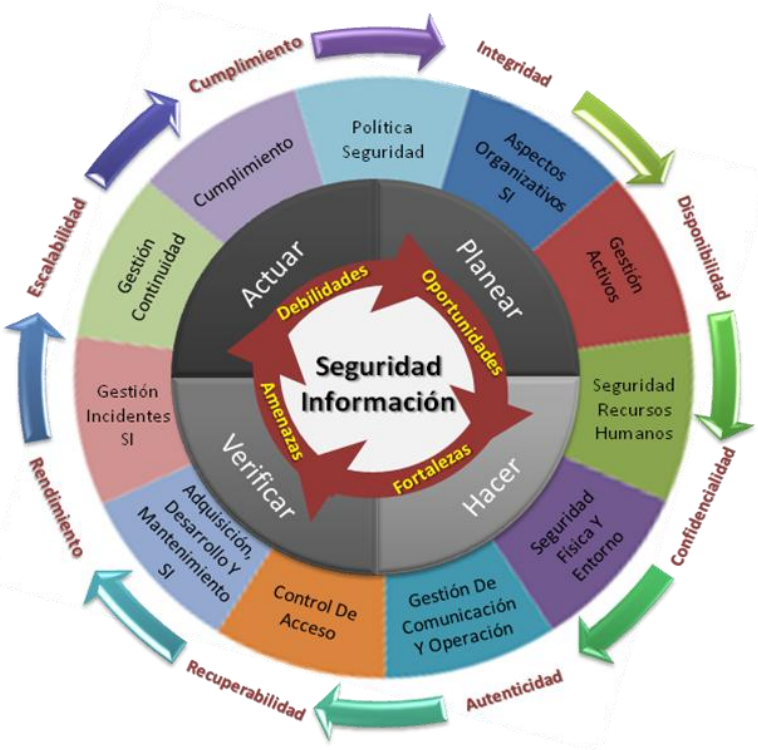
Como indica Luis Fuertes [9] “Los riesgos informáticos pueden estar relacionados con la pérdida potencial de información y la recuperación de dichos datos, o bien, con el uso permanente de la información”; estas acciones abarcan las siguientes categorías:

- ***Integridad***: es el riesgo que se genera cuando la información no está completa, precisa, ni protegida contra cambios no autorizados o puede ser alterada o utilizada por personas no autorizadas, por ejemplo, delitos informáticos, infracciones internas, terrorismo electrónico. [9], [10]
- ***Disponibilidad***: riesgo que se produce por la imposibilidad de acceder a la información cuando, por ejemplo, se produce un fallo en el sistema debido a, entre otras cosas, cambios en la configuración, falta de redundancia en las arquitecturas informáticas, o errores humanos. [10]
- ***Confidencialidad***: Riesgo que se presenta Cuando la información está disponible para personas No autorizadas.[10]
- ***Autenticidad***: Riesgo que se crea cuando no hay confiabilidad en el intercambio de información entre ubicaciones diferentes.[9]
- ***Recuperabilidad***: riesgo que se genera cuando la información necesaria o vital no puede recuperarse en un tiempo prudente después de un incidente relacionado con la seguridad o la disponibilidad debido a , por ejemplo, fallos en hardware y/o en software, amenazas externas, o desastres naturales.[9]
- ***Rendimiento***: riesgo que se crea cuando la información necesaria no puede suministrarse debido a, entre otros factores, arquitecturas distribuidas, picos en la demanda, o heterogeneidad en el entorno de las SI/TI. [9]
- ***Escalabilidad***: riesgo que se produce cuando las principales nuevas fuentes de demanda de información (nuevas aplicaciones, nuevas líneas de negocio) no pueden manejarse de forma rentable debido, principalmente, a crecimiento del volumen de negocio, cuellos de botella en el suministro, o a arquitecturas aisladas.[9]
- ***Cumplimiento:*** riesgo que se genera cuando la gestión o el uso de la información infringe los requisitos normativos. Por ejemplo, normativas gubernamentales, pautas de la dirección corporativa o políticas internas”.[9]

El gráfico que se presenta a continuación muestra el ciclo de mejora continua de la seguridad de la información, interrelacionando los controles de SI de la 27002 con el modelo PDCA, el análisis FODA y los factores de SI, en forma cíclica a fin de afianzar las actividades de la organización controlando los riesgos.

Se debe estar en constante observación del entorno y de los aspectos que afectan la seguridad de los activos informáticos de la organización tanto a nivel interno como externo a fin de que este ciclo no se vea interrumpido.

Figura 5. Ciclo de Mejora continua de la Seguridad de la Información



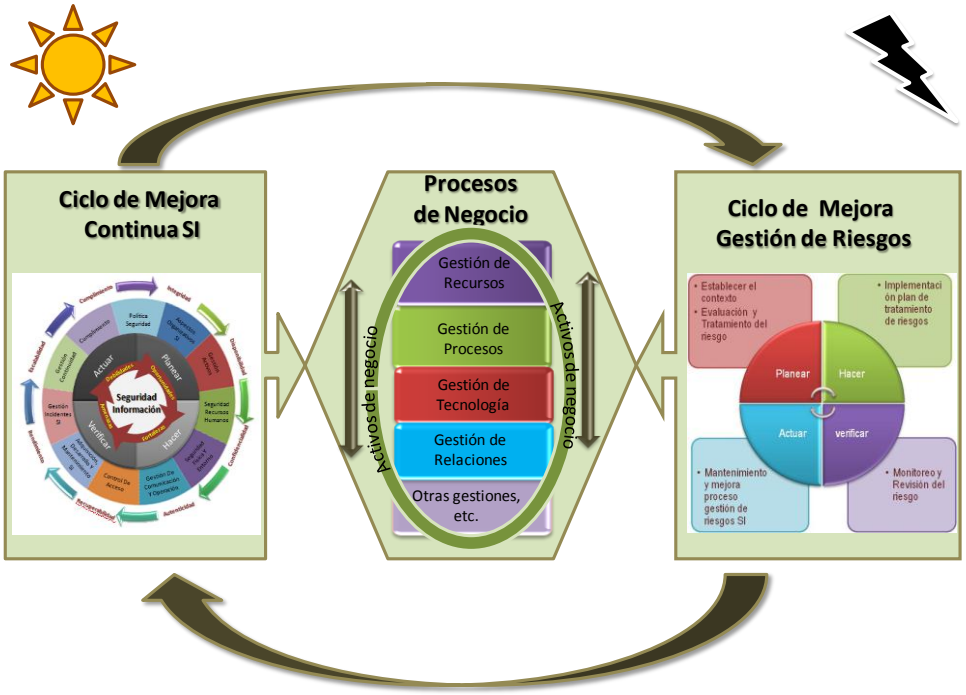
El gráfico muestra como núcleo la seguridad de la información, en un entorno de análisis FODA y círculo de Demming para realizar una mejora continua a todos los aspectos de control de seguridad de la información de la ISO/IEC 27002 y teniendo en cuenta las 8 categorías o criterios de manejo de la información.

CAPITULO 4
GUIA PARA GESTIONAR LOS RIESGOS DE SEGURIDAD DE LA INFORMACION EN TIEMPOS DE CRISIS

En el capítulo 1 se ha explicado el contexto de las Crisis, en el capítulo 2, los conceptos y proceso gestión de riesgos, en el capítulo 3 se describieron los conceptos y la importancia de gestionar la seguridad de información, con eje en la gestión de riesgos. También se enumeraron las principales normas y estándares referidos a estos conceptos.

Ahora bien, como se indicó en el primer capítulo, las unidades del negocio pueden ser generadoras de crisis o ser afectadas por ellas, y es ante estas situaciones en donde hay que hacer especial énfasis para gestionar la seguridad.

Figura 6. Interrelación óptima entre los procesos de negocio, sus activos, el SGR y el SGSI



El gráfico 6 muestra como el ciclo de vida de seguridad de la información y la gestión de riesgos están ligados a los procesos de negocio.

Estos requieren de activos, los cuales están expuestos a amenazas en función de sus vulnerabilidades. Es necesario administrar los riesgos sobre los activos, y en particular, gestionar los riesgos que puedan afectar a la seguridad de la información, siendo esta uno de sus activos más importantes para la continuidad del negocio. EL objetivo de este círculo virtuoso es mantener el equilibrio en la organización. Los riesgos deben ser medidos y evaluados de manera periódica para mejorar los puntos débiles, afianzar las fortalezas, contrarrestar las amenazas del entorno y aprovechar las oportunidades que puedan dar valor al negocio.

4.1. Enfoque Metodológico Para Gestionar Los Riesgos En Tiempos De Crisis

A continuación se detallan los aspectos relevantes referidos a riesgos de seguridad de la información, que sirven como guía práctica para gestionar estos riesgos en tiempo de crisis.

Como dinámica se utilizan cuadros de preguntas con los aspectos organizacionales, sobre los cuales la alta gerencia debe cuestionarse, y tomar decisiones que conlleven acciones que mejoren los procesos de manera de no entrar en momentos críticos.

Dentro de las actividades diarias para cualquier área o puesto de trabajo se deben realizar análisis, control y ejecución de actividades poniendo especial atención en las regulaciones impuestas por la compañía para el desarrollo y gestión de las mismas, creando cultura organizacional de seguridad y mitigación del riesgo. Los siguientes cuestionarios permitirán incursionar en ese análisis para encontrar y medir los aspectos claves de riesgos.

Adicionalmente se tienen en cuenta algunas preguntas del documento “Managing risk in perilous times - Practical steps to accelerate recovery” [8], ajustados con lo ya descrito en los capítulos anteriores, teniendo en cuenta las variables de la ISO/IEC 27002 así como el aporte personal de la

experiencia y de lo aprendido a lo largo del relevamiento bibliográfico realizado para el desarrollo de este trabajo.

A continuación se presenta una tabla que sirve para concienciar a la alta gerencia sobre las debilidades que tiene la organización respecto de los riesgos de seguridad de la información y de los controles que se han implementado para ayudar a prevenirlos.

Tabla 1. Cuestionario de generalidades de Riesgos y SI

Preguntas Generales	Controles ISO/IEC-27002	Áreas que intervienen
✓ ¿hay concientización y cultura de seguridad jerarquizado en todo el personal de la organización? ✓ ¿Sabe Qué está pasando? ✓ ¿Cómo lo está controlando? ✓ ¿Como lo está midiendo? ✓ ¿Quién es el responsable de los controles y mediciones? ✓ ¿Está realizando estadísticas? ✓ ¿con que periodicidad? ✓ ¿existen políticas de manejo y control? ✓ ¿Conoce los aspectos de seguridad de su organización, como aplicarlos y hacer que se cumplan? ✓ ¿Si está cumpliendo con lo establecido en que se beneficia? ✓ ¿Si no cumple en que le puede afectar? ✓ ¿Cuál es el costo - beneficio en el corto, mediano y largo plazo si cumple o no? ✓ ¿Tiene claridad del impacto y probabilidad de ocurrencia de las posibles eventualidades que llegasen a suceder? ✓ ¿Conoce y tiene cómo contrarrestar las posibles eventualidades? ✓ ¿Sabe qué hacer? ✓ ¿Puede hacerlo? ✓ ¿Sabe Cuando hacerlo? ✓ ¿Sabe Cómo hacerlo? ✓ ¿A quién le corresponde hacerlo? ✓ ¿Cuenta con personal calificado para hacerlo? ✓ ¿cuenta con los recursos e infraestructura adecuada para hacerlo? ✓ ¿Tiene las herramientas y conocimientos organizacionales para manejar una crisis?	1. Política De Seguridad. 2. Aspectos Organizativos De La Seguridad De La Información. 3. Gestión De Activos. 4. Seguridad Ligada A Los Recursos Humanos. 5. Seguridad Física Y Del Entorno. 6. Gestión De Comunicaciones Y Operaciones. 7. Control De Acceso. 8. Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información 9. Gestión De Incidentes En La Seguridad De La Información. 10. Gestión De La Continuidad Del Negocio. 11. Cumplimiento.	➢ Alta Gerencia ➢ Riesgos ➢ Seguridad de Información ➢ TI ➢ Recursos Humanos ➢ Operaciones ➢ Financiera

Es importante que las gerencias realicen estos cuestionarios a fin de que las preguntas realizadas en ellos ayuden a las organizaciones a tener en cuenta diferentes criterios para medir y controlar los riesgos de manera periódica, mejorando así debilidades a fin de dar solidez a la funcionalidad y operatividad de las actividades propias de la empresa.

Una vez conocidos los aspectos generales de la organización, los recursos con que cuenta y las actividades a realizar, se puede de manera específica realizar un análisis de riesgos a los controles de seguridad midiendo las causas y efectos relevantes para un buen manejo de las crisis. Para facilitar esto a continuación se ha incluido una segunda tabla con un cuestionario de preguntas que tienen como fin evaluar aspectos específicos a la seguridad de la información.

Tabla 2. Cuestionario de aspectos específicos sobre los controles de SI para gestionar los riesgos:

Controles **ISO/IEC 27002**	**Gestión de Riesgos:** **Evaluar las causas y efectos de cada pregunta**
Política de seguridad de la información. ✓ Documento de política de seguridad de la información. ✓ Revisión de la política de seguridad de la información.	✓ ¿Se tiene una política de seguridad? ✓ ¿Cómo controla el cumplimiento de la política? ✓ ¿existe un plan de seguridad? ✓ ¿Si tiene un plan de seguridad como le está beneficiando? ✓ ¿La divulgación del plan de seguridad y el cumplimiento del mismo como le beneficia? ✓ ¿En el plan de seguridad, están implementados y actualizados los controles y estadísticas de gestión de seguridad y de riesgos? ✓ ¿Es de conocimiento de toda la organización la existencia y funcionalidad del plan de seguridad? ¿Existe un comité para manejo de seguridad? ✓ ¿Se realizan controles de impacto y medición de riesgo para la seguridad de la información? ✓ ¿Se conocen las áreas críticas de la organización y su medición de riesgo para la seguridad de la información y funcionalidad del negocio? ✓ ¿Se conoce la forma de contrarrestar los riesgos que afectan la seguridad de la información?

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
Aspectos Organizativos De La Seguridad De La Información. **Organización interna.** ✓ Compromiso de la Dirección con la seguridad de la información. ✓ Coordinación de la seguridad de la información. ✓ Asignación de responsabilidades relativas a la seg. de la informac. ✓ Proceso de autorización de recursos para el tratamiento de la información ✓ Acuerdos de confidencialidad. ✓ Contacto con las autoridades. ✓ Contacto con grupos de especial interés. ✓ Revisión independiente de la seguridad de la información.	✓ ¿existe compromiso de seguridad por parte de los directivos de la organización? ✓ ¿La dirección aporta a la seguridad de manera objetiva y ágil? ✓ ¿Existe compromiso de todo el personal a la seguridad información y el uso de buenas prácticas y cómo le está beneficiando? ✓ ¿Existe dentro de la organización un responsable de la seguridad? ✓ ¿Cómo interactúa el responsable de seguridad con el personal de la organización? ✓ ¿Hay buenas relaciones entre el responsable de seguridad, el responsable de TI y el responsable de riesgos? ✓ ¿Los profesionales de riesgo tienen autoridad competente en la organización, si surge un problema potencial con consecuencias perjudiciales para la reputación? ✓ ¿hay confianza en los procesos en marcha, tienen contemplado el tipo de riesgo y su impacto para ser elevados a la dirección ejecutiva? ✓ ¿Se tiene claridad del impacto y probabilidad de ocurrencia de las posibles eventualidades que llegasen a suceder y cuál es su manejo dentro de la organización? ✓ ¿Al escalar a la dirección ejecutiva los resultados de la evaluación de los procesos contribuyen a un mejoramiento continúo? ✓ ¿A quién le corresponde hacer gestión de riesgos, y que mecanismos está utilizando para contrarrestar los riesgos? ✓ ¿Las estrategias de negocio se actualizan periódicamente teniendo en cuenta la gestión de riesgos y su aporte? ✓ ¿Centralizar los riesgos le beneficia? ✓ ¿Está evaluando el entorno constantemente, esto en que lo beneficia? ✓ ¿los controles que realiza son los adecuados para su organización? ✓ ¿cuenta con personal calificado para realizar las mediciones? ✓ ¿Las estadísticas e indicadores que lleva son los indicados para la organización?

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
	✓ ¿Los periodos de evaluación son constantes y son relevantes para la organización? ✓ ¿La empresa tiene establecido un equilibrio adecuado entre la autoridad de gestión del riesgo y el beneficio en la toma de objetivos? ✓ ¿Cuál es la posición de la gestión de riesgos en la organización? ✓ ¿Qué tan cerca están los riesgos del negocio? ✓ ¿En qué medida la gestión del riesgo es un apoyo a la función del negocio? ✓ ¿Si la gestión de riesgos tiene una relación de integración estrecha con el negocio, esto lleva a realizar un papel más estratégico? ✓ ¿De qué manera podría dar beneficio a la organización la identificación y centralización de los riesgos, sujeto a un punto de vista de toda la empresa? ✓ ¿Con qué frecuencia la organización hace revisión y la actualización de sus supuestos sobre el riesgo del entorno? ✓ ¿Es este proceso lo suficientemente frecuente dada las actuales condiciones externas y el impacto de las mismas? ✓ ¿Cómo es la información sobre el riesgo si llegase a cambiar las condiciones del entorno? ✓ ¿esto se comunica a la alta dirección, y en qué contribuye? ✓ ¿En qué medida los cambios en el riesgo externo y cambios del entorno conducen a cambios en la gestión de riesgos, prioridades o procesos?
Terceros. Identificación de los riesgos derivados del acceso de terceros. Tratamiento de la seguridad en la relación con los clientes. Tratamiento de la seguridad en contratos con terceros.	✓ ¿existen políticas de manejo y control de terceros? ✓ ¿Quién es responsable de las actividades desarrolladas por estos? ✓ ¿El responsable del control de terceros está capacitado y tiene la experiencia y experticia para esta labor? ✓ ¿Cómo se maneja el aspecto de seguridad de la información respecto de los terceros?
Gestión De Activos. **Responsabilidad sobre los activos**. ✓ Inventario de activos. ✓ Propiedad de los activos.	✓ ¿Existen políticas de manejo y control de activos? ✓ ¿Se realiza control de activos?

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
✓ Uso aceptable de los activos. **Clasificación de la información.** ✓ Directrices de clasificación. ✓ Etiquetado y manipulado de la información.	✓ ¿Quién es el encargado de los activos informáticos de la organización? ✓ ¿Están clasificados los activos? ✓ ¿Se conocen los riesgos implícitos dentro de la gestión de activos? ✓ ¿Sabe cómo contrarrestar los riesgos de activos?
Seguridad Ligada A Los Recursos Humanos: **Antes del empleo**. ✓ Funciones y responsabilidades. ✓ Investigación de antecedentes. ✓ Términos y condiciones de contratación. **Durante el empleo.** ✓ Responsabilidades de la Dirección. ✓ Concientización, formación y capacitación en seguridad de la información. ✓ Proceso disciplinario. **Cese del empleo o cambio de puesto de trabajo.** ✓ Responsabilidad del cese o cambio. ✓ Devolución de activos. ✓ Retirada de los derechos de acceso.	✓ ¿Está realizando controles de ingreso del personal, conoce su perfil, su nivel de compromiso y el grado de confianza que puede depositar en ellos? ✓ ¿Quién es el responsable de los controles y mediciones? ✓ ¿Existen políticas de manejo y control de recursos humanos? ✓ ¿Existe definición de roles y perfiles por cargo? ✓ ¿Existen criterios y manejos de Integridad, ética, competencias, y responsabilidad del personal? ✓ ¿Hay cultura de entrega de valor y gestión de riesgos? ✓ ¿Existen manuales internos de funciones, procesos y procedimientos? ✓ ¿Están actualizados estos manuales? ✓ ¿El personal es calificado y puedo contar con ellos cuando lo necesite? ✓ ¿Se cuenta con personal idóneo y de confianza para realizar esta labor? ✓ ¿Las políticas se ajustan a las condiciones actuales de la organización? ✓ ¿Los roles y perfiles están actualizados y ajustados con los cargos definidos? ✓ ¿Están definidos los valores éticos y organizacionales, se están cumpliendo? ✓ ¿El personal está comprometido con la política de Seguridad de Información y contribuye a su gestión? ✓ ¿El personal está comprometido con la política de riesgos y contribuye a su gestión? ✓ ¿Están definidos y actualizados los manuales y el personal los pone en práctica? ✓ ¿Están definidos los riesgos y prioridades, por cargo, por proceso o por procedimiento? ✓ ¿Quién está midiendo los riesgos y con qué periodicidad actualiza indicadores? ✓ ¿Está el equipo de liderazgo capacitado para brindar

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
	una adecuada orientación para establecer las expectativas en torno a los riesgos gestión? ✓ ¿Existen comités independientes para revisar las prácticas de gestión de riesgos? ¿Es esto apropiado? ✓ ¿Hay alguna persona en la organización con la responsabilidad general de la gestión del riesgo? ✓ ¿Son los procesos de gobierno corporativo suficientemente sólidos en la organización para asegurarse de que los inconvenientes de remuneración no causará problemas a la reputación?[8] ✓ ¿Hay una remuneración calificada, existe un comité para revisar y aprobar las políticas?[8] ✓ ¿Cómo es la relación entre el rendimiento corporativo y la compensación? [8] ✓ ¿Los indicadores los adecuados? ✓ ¿Están siendo utilizados los indicadores en toda la organización? ✓ ¿Existen programas de incentivos diseñados de tal manera que motivan y recompensan, para no fomentan una conducta perjudicial a largo plazo a los intereses de los accionistas? [8] ✓ ¿En caso de una eventualidad en que me beneficia tener actualizados los manuales por cargo? ✓ ¿Se cuenta con personal idóneo y de confianza para gestionar los riesgos en una eventualidad y dar continuidad al negocio? ✓ El manejo y comunicación de los riesgos es el adecuado
Seguridad Física Y Del Entorno. **Áreas seguras.** ✓ Perímetro de seguridad física. ✓ Controles físicos de entrada. ✓ Seguridad de oficinas, despachos e instalaciones. ✓ Protección contra las amenazas externas y de origen ambiental. ✓ Trabajo en áreas seguras. ✓ Áreas de acceso público y de carga y descarga. **Seguridad de los equipos.** ✓ Emplazamiento y protección de	✓ ¿Cuáles son los principales riesgos que enfrenta la organización? ✓ ¿Tiene usted plena confianza en que el ejecutivo gestión de riesgos, es consciente de los riesgos los conoce, los identifica, en cuanto a la gravedad y el impacto potencial que podrían tener en el negocio?[8] ✓ ¿El equipo de dirección ejecutiva en la organización contiene a personas de un conjunto diverso de experiencia profesional? [8] ✓ ¿Hay peligro de que los altos ejecutivos puedan ser aislados de la comprensión de la imagen de verdadero riesgo, porque la información se filtra en medida que se eleva la jerarquía?[8] ✓ ¿Tiende la organización a comprender la interacción entre las diferentes categorías de riesgo y la forma en que un evento en una parte de la empresa podría

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
equipos. ✓ Instalaciones de suministro. ✓ Seguridad del cableado. ✓ Mantenimiento de los equipos. ✓ Seguridad de los equipos fuera de las instalaciones. ✓ Reutilización o retirada segura de equipos. ✓ Retirada de materiales propiedad de la empresa.	tener un efecto en cadena en otras partes?[8] ✓ ¿Existe un lenguaje común de riesgo para asegurar la claridad de la comprensión a través de la organización?[8] ✓ ¿La organización tiene una base de datos y de TI infraestructura que soporta la agregación y comunicación de información sobre los riesgos?[8]
Gestión De Comunicaciones Y Operaciones. **Responsabilidades y procedimientos de operación.** ✓ Documentación de los procedimientos de operación. ✓ Gestión de cambios. ✓ Segregación de tareas. ✓ Separación de los recursos de desarrollo, prueba y operación. **Supervisión.** ✓ Registros de auditoría. ✓ Supervisión del uso del sistema. ✓ Protección de la información de los registros. ✓ Registros de administración y operación. ✓ Registro de fallos. ✓ Sincronización del reloj. **Gestión de la provisión de servicios por terceros.** ✓ Provisión de servicios. ✓ Supervisión y revisión de los servicios prestados por terceros. ✓ Gestión del cambio en los servicios prestados por terceros. **Planificación y aceptación del sistema.** ✓ Gestión de capacidades.	✓ ¿Cuáles son las fuentes de información que la organización utiliza para obtener una comprensión de sus riesgos y cual su posición? [8] ✓ ¿Qué tan confiables son estas fuentes y se pusieron a prueba frente a otras fuentes para asegurar su validez? [8] ✓ ¿La organización tienden a basarse en la experiencia histórica de los datos? ✓ ¿Hasta qué punto va el juicio humano y el instinto que están siendo utilizados como un método para identificar y evaluar el riesgo? [8] ✓ ¿Para generar confianza la organización está aplicando la combinación correcta de insumos de riesgo cualitativo y cuantitativo? [8] ✓ ¿La gerencia se reserva un tiempo para analizar los posibles escenarios políticos y económicos, y considera el impacto de estos resultados en el negocio? [8] ✓ Si no es así, ¿se debe hacer de manera más formal? ✓ ¿Hasta qué punto son considerados diferentes escenarios a la hora de establecer estrategias a largo plazo? [8] ✓ ¿Existe una tendencia de confiar en un oficial de cumplimiento, en lugar de la prueba modelo de negocio frente a otros resultados potenciales? [8] ✓ ¿La gerencia senior busca una gama de diferentes puntos de vista y diferentes perspectivas, con el fin de poner a prueba sus hipótesis? [8] ✓ ¿Hasta qué punto la organización se basa en fuentes externas de información sobre los riesgos? [8] ✓ ¿Cómo es la información que tiene la organización, que tan robusta es la regularidad de referencia con otras fuentes? [8] ✓ ¿La organización conoce y comprende la

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
✓ Aceptación del sistema. **Protección contra el código malicioso y descargable.** ✓ Controles contra el código malicioso. ✓ Controles contra el código descargado en el cliente. **Copias de seguridad.** ✓ Copias de seguridad de la información	metodología detrás de las fuentes externas de la información que se utiliza? [8] ✓ ¿existen copias de seguridad de la información? ✓ ¿Quien realiza estas copias? ✓ ¿Se tiene un proceso controlado de las copias y su archivo? ✓ ¿Existe conciencia de las limitaciones de estos datos?
Gestión de la seguridad de las redes. ✓ Controles de red. ✓ Seguridad de los servicios de red.	✓ ¿Se controla la red? ✓ ¿Cómo se controlan los servicios a través de la red? ✓ ¿Son seguros los servicios que están en la red?
Manipulación de los soportes. ✓ Gestión de soportes extraíbles. ✓ Retirada de soportes. ✓ Procedimientos de manipulación de la información. ✓ Seguridad de la documentación del sistema.	✓ ¿Existen políticas de manejo y control de soportes? ✓ ¿Se conocen los procedimientos de manipulación de información? ✓ ¿Existe control de la documentación del sistema?
Intercambio de información. ✓ Políticas y procedimientos de intercambio de información. ✓ Acuerdos de intercambio. ✓ Soportes físicos en tránsito. ✓ Mensajería electrónica. ✓ Sistemas de información empresariales.	✓ ¿Existen políticas de procedimientos para manejo y control de intercambio de información? ✓ ¿Se cuenta con personal calificado para la realización de estos controles? ✓ ¿Se conocen los riesgos de intercambio de información y sabe como contrarrestarlos?
Servicios de comercio electrónico. ✓ Comercio electrónico. ✓ Transacciones en línea. ✓ Información públicamente disponible.	✓ ¿Se evalúa el crecimiento y mejoramiento de la gestión de Servicios como un sistema de control cerrado; como aumento del potencial de servicio y desempeño; demanda, capacidad y costo? [8] ✓ ¿Evalúa la gestión financiera cuantifica en términos financieros el valor de los servicios de TI y de los activos utilizados para su entrega y calcula las previsiones futuras? [8] ✓ ¿Se considera la alineación de los servicios existentes con los objetivos del negocio; el uso de sus recursos y capacidades, y las opciones para

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
	modificaciones? ✓ ¿Se tiene en cuenta que la gestión de capacidad, asegure la capacidad instalada existente en todas las áreas de TI justifica los costos y las necesidades presentes y futuras están de acuerdo con las necesidades del negocio en forma oportuna?[8] ✓ ¿Se evalúa la gestión de la disponibilidad de los servicios de TI? ✓ ¿Se tiene en cuenta toda la información de la gestión de la seguridad de la información almacenada en el sistema de gestión de seguridad de información a fin de que cubra todos los servicios de TI y sus componentes?[8]
Control De Acceso: **Requisitos de negocio para el control de acceso.** ✓ Política de control de acceso. **Gestión de acceso de usuario.** ✓ Registro de usuario. ✓ Gestión de privilegios. ✓ Gestión de contraseñas de usuario. ✓ Revisión de los derechos de acceso de usuario. **Responsabilidades de usuario.** ✓ Uso de contraseñas. ✓ Equipo de usuario desatendido. ✓ Política de puesto de trabajo despejado y pantalla limpia. **Control de acceso a la red.** ✓ Política de uso de los servicios en red. ✓ Autenticación de usuario para conexiones externas. ✓ Identificación de los equipos en las redes. ✓ Protección de los puertos de diagnóstico y configuración remotos. ✓ Segregación de las redes. ✓ Control de la conexión a la red.	✓ ¿Existe una política de manejo y control de accesos? ✓ ¿Existen normas y procedimientos que apoyen a esta política? ✓ ¿Se lleva registro de usuarios? ✓ ¿Se han definido privilegios de acceso: de usuario, a la red, a los sistemas operativos, a las aplicaciones, a los ordenadores, portátiles y USB? ✓ ¿Se han identificado y se piensa continuar identificando los riesgos de control de accesos? ✓ ¿Se sabe como contrarrestar estos riesgos? ✓ ¿Se tiene cultura organizacional de responsabilidad para los controles de acceso? ✓ ¿Se cuenta con personal calificado para controlar los accesos? ✓ ¿Existe un responsable de los controles de acceso? ✓ ¿Se conoce la política de uso de los servicios de red? ✓ ¿Se actualiza la política y se tienen controles para su aplicabilidad? ✓ ¿Existen restricciones de acceso a la red? ✓ ¿Existen controles para las restricciones de conexiones externas? ✓ ¿Se tiene identificados los equipos que están en la red? ✓ ¿Se encuentran segregación de las redes? ✓ ¿Existen controles de conexión en la red?

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
✓ Control de encaminamiento (routing) de red. **Control de acceso al sistema operativo.** ✓ Procedimientos seguros de inicio de sesión. ✓ Identificación y autenticación de usuario. ✓ Sistema de gestión de contraseñas. ✓ Uso de los recursos del sistema. ✓ Desconexión automática de sesión. ✓ Limitación del tiempo de conexión. **Control de acceso a las aplicaciones y a la información.** ✓ Restricción del acceso a la información. ✓ Aislamiento de sistemas sensibles. **Ordenadores portátiles y teletrabajo.** ✓ Ordenadores portátiles y comunicaciones móviles. ✓ Teletrabajo.	✓ ¿Existen controles de encadenamiento de la red? ✓ ¿Existen controles de seguridad a los procedimientos de inicio de sesión? ✓ ¿Existen controles de identificación y autenticación de los usuarios? ✓ ¿Se conoce el sistema de gestión de contraseñas?, esta implementado?, Que controles realiza para verificar que se cumple? ✓ ¿Se conocen los usos de los recursos del sistema? ✓ ¿Se tienen establecidos controles de desconexión y limitaciones de tiempo de las conexiones? ✓ ¿Se tienen controles de acceso a la información? ✓ ¿Se realiza gestión para el aislamiento de los sistemas sensibles? ✓ ¿Se tienen controles de ordenadores portátiles, comunicaciones móviles y teletrabajo? ✓ ¿Cómo realiza el seguimiento de estos controles? ✓ ¿Conoce las vulnerabilidades técnicas? ✓ ¿Qué hace para contrarrestar el efecto negativo que pueda llegar a ocasionar?
Adquisición, Desarrollo Y Mantenimiento De Sistemas De Información **Requisitos de seguridad de los sistemas de información.** ✓ Análisis y especificación de los requisitos de seguridad. **Tratamiento correcto de las aplicaciones**. ✓ Validación de los datos de entrada. ✓ Control del procesamiento interno. ✓ Integridad de los mensajes. ✓ Validación de los datos de salida. **Controles criptográficos.**	✓ ¿Existe una política de manejo y control de mantenimiento de los sistemas de información: aplicaciones, controles criptográficos, archivos de sistema, procesos de desarrollo y soporte? ✓ ¿Conoce las vulnerabilidades técnicas? ✓ ¿Qué hace para contrarrestar el efecto negativo que pueda llegar a ocasionar? ✓ ¿Qué tipo de controles realiza a las aplicaciones y el acceso a las mismas?, ¿Como las mide? ✓ ¿Quién es el responsable de realzar esta labor? ✓ ¿Qué controles criptográficos realiza y como los mide? ✓ ¿Cómo controla la seguridad de los archivos de sistema? ✓ ¿Qué tipo de controles realiza para dar seguridad a los procesos de desarrollo y soporte?,

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
✓ Política de uso de los controles criptográficos. ✓ Gestión de claves. **Seguridad de los archivos de sistema.** ✓ Control del software en explotación. ✓ Protección de los datos de prueba del sistema. ✓ Control de acceso al código fuente de los programas. **Seguridad en los procesos de desarrollo y soporte.** ✓ Procedimientos de control de cambios. ✓ Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo ✓ Restricciones a los cambios en los paquetes de software. ✓ Fugas de información. ✓ Externalización del desarrollo de software. **Gestión de la vulnerabilidad técnica.** ✓ Control de las vulnerabilidades técnicas.	✓ ¿Cómo controla los riesgos que se generan en los procesos de desarrollo y soporte, para software propio y software tercerizado? ✓ ¿Existe un sistema de gestión de claves? ✓ ¿Se tienen identificados los controles de seguridad de los archivos de sistema? ¿Cómo se controlan? ✓ ¿Existe un responsable de estos controles? ✓ ¿Existe gestión de seguridad en los procesos de desarrollo y soporte? ✓ ¿Cómo maneja los procedimientos de control de cambios? ✓ ¿Qué tipo de revisiones técnicas y seguimiento realiza? ✓ ¿Qué tipo de controles y restricciones realiza para evitar fugas de información? ✓ ¿Se conoce las vulnerabilidades técnicas? ✓ ¿Qué hace para contrarrestar el efecto negativo que pueda llegar a ocasionar?
Gestión de Incidentes de seguridad de la información **Notificación de eventos y puntos débiles de seguridad de la información** ✓ Notificación de los eventos de seguridad de la información. ✓ Notificación de puntos débiles de seguridad. **Gestión de incidentes y mejoras de seguridad de la información.** ✓ Responsabilidades y procedimientos. ✓ Aprendizaje de los incidentes de seguridad de la información.	✓ ¿Existe una política para manejo y control de incidentes? ✓ ¿Se conocen los eventos y puntos débiles de la seguridad? ✓ ¿Sabe cómo controlar las debilidades y su efecto negativo? ✓ ¿Cuenta con los recursos necesarios para solucionar los incidentes? ✓ ¿Existe un responsable del control de incidentes? ✓ ¿tiene mediciones y estadísticas de incidentes? ✓ ¿Realiza retroalimentación de los incidentes presentados, evaluándolos y controlándolos para que

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
✓ Recopilación de evidencias.	no se vuelvan a repetir? ✓ ¿Recopila las evidencias de los incidentes? ¿en lo benéfica esta labor?
Gestión De La Continuidad Del Negocio. **Aspectos de seguridad de la información en la gestión de la continuidad del negocio.** ✓ Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio. ✓ Continuidad del negocio y evaluación de riesgos. ✓ Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información. ✓ Marco de referencia para la planificación de la cont. del negocio. ✓ Pruebas, mantenimiento y reevaluación de planes de continuidad.	✓ ¿Tiene una política de manejo y control de gestión a la continuidad del negocio? ✓ ¿La estructura organizacional apoyará la implementación de la estrategia? ✓ ¿Las responsabilidades de la gestión de riesgos están integradas en la organización? ✓ ¿Existe infraestructura que facilite y apoye la creación y el intercambio de información comercial vital? ✓ ¿Se han comunicado las estrategias y los objetivos de manera efectiva a todos los que necesitan saber en la organización? [4] ✓ ¿Se sabe cómo dar continuidad al negocio desde una perspectiva global a la operativa de la organización? ✓ ¿Se tiene en cuenta la gestión de la continuidad del servicio de TI y se apoya en la gestión de la continuidad del negocio, asegurando que todos los requerimientos técnicos de TI y servicios instalados puedan reanudarse en los plazos acordados?[4] ✓ ¿La gestión de la continuidad del servicio de TI es esencial para asegurar la continuidad del negocio; objetivos, alcance y valor; enfoque del ciclo de vida de la gestión de la continuidad del servicio de TI? [4] ✓ ¿Se desarrolla planes de gestión de la continuidad del servicio de TI en coordinación con los planes para: respuestas a emergencias, evaluación de daños, rescates, registros vitales, gestión de crisis y relaciones públicas, alojamiento y servicios, seguridad, personal, comunicaciones, administración y finanzas; plan organizacional; pruebas? [4] ✓ ¿Se realizan análisis de impacto en el negocio; registro de riesgo; estrategia de gestión de continuidad del negocio y planes de continuidad de negocio; detalles y cronogramas de pruebas; planes de gestión de la continuidad del servicio de TI; planes relacionados; toda la información relacionada con la recuperación; toda la información de respaldo y recuperación? [4]
Cumplimiento. **Cumplimiento de los requisitos legales.** ✓ Identificación de la legislación aplicable. ✓ Derechos de propiedad intelectual	✓ ¿Se conocen las normas y legislaciones que lo regulan? ✓ ¿Se da cumplimiento a los mismos?

Controles ISO/IEC 27002	Gestión de Riesgos: Evaluar las causas y efectos de cada pregunta
(DPI). ✓ Protección de los documentos de la organización. ✓ Protección de datos y privacidad de la información de carácter personal ✓ Prevención del uso indebido de recursos de tratamiento de la información ✓ Regulación de los controles criptográficos. **Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.** ✓ Cumplimiento de las políticas y normas de seguridad. ✓ Comprobación del cumplimiento técnico. **Consideraciones sobre las auditorías de los sistemas de información.** ✓ Controles de auditoría de los sistemas de información. ✓ Protección de las herramientas de auditoría de los sistemas de información.	✓ ¿Se realizan controles de cumplimiento legal, técnico y de auditoría? ✓ ¿Quién es el responsable de llevar estos controles? ✓ ¿Cómo se protege la información de carácter personal? ✓ ¿Existe prevención de los usos indebidos de los recursos de tratamiento de la información? ✓ ¿Se conoce y se maneja regulaciones de controles criptográficos? ✓ ¿Existe cumplimiento de las políticas y normas de seguridad y cumplimiento técnico? ✓ ¿Se conocen las vulnerabilidades de cumplimiento técnico? ✓ ¿Qué hace para contrarrestar el efecto negativo que pueda llegar a ocasionar? ✓ ¿Se conocen y se tienen identificados los controles y consideraciones de las auditorias de sistemas de información? ✓ ¿Cómo protege las herramientas de auditoría de los sistemas de información?

Una vez realizado el análisis de causa y efecto de los riesgos referidos a aspectos de la seguridad, se deben tener ciertas recomendaciones que den valor a la organización a fin de realizar mejores prácticas. A continuación se dan algunas recomendaciones, como aporte propio del tema investigado, y se presentan las conclusiones finales, en base al objetivo planteado.

CONCLUSIONES Y RECOMENDACIONES

Las conclusiones y recomendaciones que se enuncian a continuación están expresadas en base a mejores prácticas que pueden contribuir para un buen manejo de los procesos, recursos y demás aspectos de la organización en los tiempos de crisis; estos están enmarcados dentro del contexto de mantener la gestión de riesgos y los aspectos de seguridad de la información identificados y controlados.

- Las empresas, a fin de contrarrestar el efecto de las crisis pueden desarrollar mejores prácticas dentro de una cultura organizacional, así podrán enfrentar las crisis con mayor entereza y decisión; los líderes deben conocer los puntos estratégicos, identificando los eslabones débiles y las fortalezas frente al entorno, esto le permitirá a la organización enfrentar los momentos de crisis con eficiencia y eficacia, para crecer, y dar continuidad al negocio.

- Los líderes organizacionales pueden aprovechar las crisis para que, con iniciativa, inventiva, practicidad y elocuencia se pueda generar valor agregado; ya que las crisis ayudan a tomar decisiones que permiten cambiar a favor la adversidad y traer mejoras a las empresas, sociedades y economías.

- Un buen líder investiga los detalles que generaron las crisis, ¿cómo otros manejaron estos aspectos? y aprenden de ellos, validando su propio entorno, creando indicadores, midiendo la probabilidad de ocurrencia e impacto de los hechos que le pueden afectar en la organización, Si se hace con sigilo, experticia y viveza, teniendo en cuenta la experiencia y trayectoria de la empresa, el movimiento del entorno y de la competencia, esta recomendación puede traer mayores beneficios.

- Un buen líder empresarial, si sabe manejar las crisis, puede identificar la situación más fácilmente, concentrándose en el problema y en la búsqueda de soluciones concretas, rápidas, reales y vanguardistas.

- Como líder, puede afrontar los retos de las coyunturas económicas, analizando las situaciones y sacando mayor provecho de ellas.

- La alta gerencia y líderes empresariales deben saber que no todo está escrito, y centrar su atención en conocer de las experiencias propias y de otros, para reactivar sus programas, modificándolos y adaptándolos para las crisis; así mismo pueden realizar actividades para resguardar o hacer resguardar la información importante para la continuidad del negocio.

- A su vez, la alta gerencia debe tener en cuenta el factor humano como prioridad, y así conocer quiénes son los empleados clave, quiénes están en los puestos de trabajo que son prioritarios para la organización y su continuidad. También deben buscar evitar tener una alta rotación de personal, manteniendo, controlando así posibles fugas de información; además, deben prestar atención en no dejar que los programas se vuelvan obsoletos, manteniendo actividades de monitoreo, y actualizando periódicamente los planes y programas para cuando se presenten situaciones de peligro para la organización.

- La alta gerencia debe construir momentos de confianza junto con el personal de toda la organización, creando núcleos de confianza para salvaguardar la información y mantener a flote la empresa en los momentos de crisis.

- La alta gerencia y los líderes empresariales están llamados a no dejarse vencer en las crisis; reevaluando y renovando las actividades prioritarias de la organización, que puedan ser vulnerables, y reforzando aspectos claves que les permitan crecer y fortalecerse en las crisis.

- Un buen líder empresarial debe conocer que los riesgos siempre están presentes, solo tiene que saber identificarlos y buscar mecanismos que permitan contrarrestarlos; además debe conocer cada punto o aspecto que pueda representar un riesgo, ya que estos son importantes para evaluar, entre otros, la seguridad de los activos informáticos de la organización, y crear directrices a seguir para contrarrestar su efecto nocivo, si llegase a suceder.

- Una buena opción para que las empresas puedan superar las crisis está en buscar estrategias que les permitan salvaguardar sus activos informáticos, hardware, software, bases de datos de clientes internos y externos, contar con personal calificado de principios y valores y que estén acorde con los estándares y políticas de las organizaciones, personal calificado que esté dispuesto a dar continuidad al negocio, no abandonando la organización en los momentos en que realmente necesitan de su labor y conocimiento.

- Un mecanismo que ayuda a las organizaciones a estar preparados para los momentos de peligro es implementar y mantener controles actualizados, revisar el adecuado cumplimiento de las listas de verificación y chequeo de los diferentes procesos, controlando en detalle los procedimientos y actividades claves que se deben efectuar, y ser conscientes de sus vulnerabilidades.

- Reconocer los momentos de peligro con anticipación, ayuda a la alta gerencia a estar preparados para cuando lleguen las crisis, esto contribuye a disminuir el efecto negativo, permitiendo reorientar los recursos en los aspectos que contribuyan a mejorar la situación y sacar mayor provecho de la misma.

- Para que los líderes empresariales y la alta gerencia actúen de manera objetiva en los momentos de crisis, si realizan las gestiones

preventivas explicadas a lo largo de este trabajo, pueden de manera práctica aplicar acciones reactivas (previamente definidas) para enfrentar los momentos de crisis y sacar mayor provecho de ellos, contrarrestando el efecto negativo y obteniendo un mayor beneficio.

- La alta gerencia y líderes empresariales deben evitar gestionar riesgos en el momento en que se presentan dificultades, o crisis, sin tener un análisis evaluativo previo de la organización y su entorno, ya que si no se tienen salvaguardas y controles establecidos; dicha gestión se convierte en una herramienta defensiva que no permite ver con claridad lo que está pasando, llevando a que se tomen decisiones arbitrarias, con altos costos, y gastos innecesarios, desencadenando otros hechos que pueden llegar a ser adversos para la organización.

Como conclusión final que surge de este trabajo, es muy probable que en una organización que enfrenta una crisis, sus mandos medios y altos descuiden la gestión de los riesgos y sean vulnerables a incidentes indeseables, como pueden ser los incidentes de seguridad de la información. Para minimizar esto es imprescindible prepararse, siguiendo las recomendaciones y buenas prácticas citadas.

BIBLIOGRAFÍA

Bibliografía Específica

[1] Oriol Amat, Estrategias empresariales para generar valor en tiempo de crisis, http://www.supercontable.com/oriol/articulos/13.htm. (consultada el 30/03/2012)

[2]Isaías Covarrubias, La crisis financiera y sus consecuencias, http://www.eumed.net/libros/2011c/1000/crisis.html. (consultada el 01/05/2012)

[3] Análisis de Riesgos Informáticos for Seguridad informática, http://es.scribd.com/doc/41039269/72/Analisis-de-Riesgos-Informaticos (consultada el 25/10/2011)

[4] El director, Plan Estratégico Seguridad – powerpoint, http://seguridadyseguridad.blogspot.com.ar/2009/01/plan-estrategico-seguridad-powerpoint_18.html (consultada el 18/03/2012)

[5] Deloitte, Serie Riesgo Inteligente Número 12, http://www.deloitte.com.mx/camp_institucional/docs/riesgointeligente.pdf (consultada el 25/09/2011)

[6] Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa, http://www.slideshare.net/Tabodiaz/alineando-cobit41itilv3yiso2700

(consultada el 31/01/2012)

[7] http://www.iso27000.es/iso27000.html (consultada el 31/01/2012)

[8]KPMG, Managing risk in perilous times - Practical steps, http://www.kpmg.com/cn/en/issuesandinsights/articlespublications/pages/perilous-times-eiu-200903.aspx (consultada el 05/01/2012)

[9] Luis Fuertes, Marketing Manager de Symantec., "Gestión de riesgos TI. Cómo implantar las mejores prácticas", http://www.aslan.es/boletin/boletin52/nuevoasociado.shtml

[10] Jose Luis Colom, Gestión de la Seguridad de TI, http://joseluiscolom.blogspot.com.ar/2012/04/gestion-de-la-seguridad-de-ti.html (consultada el 30/04/2012)

[11] Estándar Argentino Norma IRAM 17550 Gestión de Riesgos.

Bibliografía General

- ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems - Requirements
- ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (anterior ISO/IEC 17799:2005)
- ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management
- Johnson, M.E.; Pfleeger, S.; "Addressing Information Risk in Turbulent Times". Security & Privacy, IEEE, Jan.-Feb. 2011, page(s): 49 - 57
- NIST SP 800-39 "Gestión de Riesgos de los Sistemas de Información, una perspectiva organizacional";
- NIST SP 800-30: Guía de Gestión de Riesgos de los Sistemas de Tecnología de la Información;.
- OCTAVE: "Operationally Critical Threat, Asset, and Vulnerability Evaluation" Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT;
- http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx
- http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/Risk-IT1.aspx
- http://www.isaca.org/spanish/Pages/default.aspx

ANEXO 1: GLOSARIO DE TERMINOS

Términos y definiciones basados en la norma ISO/FDIS 31000:2009 [ISO Guide 73:2009]

1. Términos Básicos

1.1 Riesgo: Combinación de la probabilidad de un suceso y de su consecuencia.

El término "riesgo" suele utilizarse sólo en el caso de que exista, al menos, una posibilidad de consecuencia negativa.

En algunas situaciones, el riesgo surge de la posibilidad de desviación con respecto al resultado o suceso previsto.

1.2 Consecuencia: Resultado de un suceso. Se puede derivar más de una consecuencia de un mismo suceso.

Las consecuencias pueden variar de positivas a negativas. Sin embargo, las consecuencias son siempre negativas en aspectos de seguridad.

Las consecuencias se pueden expresar cualitativa o cuantitativamente.

1.3 Probabilidad: Grado en que un suceso puede tener lugar.

Definición matemática de probabilidad: "un número real situado en la escala de 0 a 1 asignado a un suceso fortuito. Puede estar relacionado con una frecuencia de ocurrencia relativa a largo plazo o con un grado de creencia de que ocurra un suceso. Para un alto grado de creencia, la probabilidad se acerca a 1".

Al describir el riesgo, se puede usar "frecuencia" en lugar de "probabilidad".

1.4 Suceso: Ocurrencia de una serie de circunstancias particulares. El suceso puede ser cierto o incierto. El suceso puede tener una sola ocurrencia o una serie de ocurrencias.

Puede calcularse la probabilidad asociada al suceso para un cierto período de tiempo.

1.5 Fuente: Elemento o actividad que disponga de un potencial de consecuencia. En el contexto de seguridad, fuente se refiere a un peligro.

1.6 Criterio de riesgos: Términos de referencia por los que se evalúa la importancia del riesgo. Los criterios de riesgo pueden incluir costos y beneficios asociados, requisitos legales y estatutarios, aspectos socioeconómicos y ambientales, las preocupaciones de los interesados, prioridades y otras aportaciones a la evaluación.

1.7 Gestión de riesgos: Actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo. La gestión de riesgos incluye, por norma general, evaluación de riesgos, tratamiento de riesgos, aceptación de riesgos y comunicación de riesgos.

1.8 Sistema de gestión de riesgos: Serie de elementos del sistema de gestión de una empresa, relacionados con la gestión de riesgos. Los elementos del sistema de gestión pueden incluir una planificación estratégica, toma de decisiones y otros procesos que traten el riesgo. La cultura de una empresa queda reflejada en su sistema de gestión de riesgos.

2 Términos Relacionados Con Personas O Empresas Afectadas Por El Riesgo

2.1 Interesado (“Stakeholder”): Cualquier individuo, grupo o empresa que pueda afectar, estar afectado por o considerarse afectado por un riesgo.

2.2 Parte interesada: Persona o grupo que tiene un interés en el resultado o éxito de una empresa. (Clientes, propietarios, personal de una empresa,

proveedores, banqueros, asociaciones, socios o sociedad). Un grupo puede comprender una empresa, una parte de esta, o más de una empresa

2.3 Percepción de riesgos: Modo en el que un interesado ve un riesgo, basándose en una serie de valores o asuntos.

La percepción del riesgo depende de las necesidades, problemas y conocimientos del interesado.

La percepción del riesgo puede diferir de los datos objetivos.

2.4 Comunicación de riesgos: Intercambio o puesta en común de información acerca del riesgo entre el encargado de la toma de decisiones y otros interesados.

La información puede estar relacionada con la existencia, naturaleza, forma, probabilidad, severidad, aceptabilidad, tratamiento y otros aspectos del riesgo.

3 Términos Relacionados Con La Valoración De Riesgos

3.1 Valoración de riesgos: Proceso general de análisis de riesgos y de evaluación de riesgos.

3.2 Análisis de riesgos: Uso sistemático de información para identificar fuentes y para calcular riesgos.

El análisis de riesgos proporciona una base para la evaluación, el tratamiento y la aceptación de riesgos.

La información puede incluir datos históricos, análisis teóricos, opiniones informadas y las preocupaciones de los interesados.

3.3 Identificación de riesgos: Proceso por el que se encuentran, enumeran y caracterizan elementos de riesgo.

Los elementos pueden incluir la fuente o peligro, suceso, consecuencia y probabilidad.

La identificación de riesgos también puede reflejar las preocupaciones de los interesados.

3.4 Identificación de fuentes: Proceso por el que se encuentran, enumeran y caracterizan fuentes.

En el contexto de seguridad, la identificación de fuentes se conoce como identificación de peligros

3.5 Estimación de riesgos: Proceso utilizado para asignar valores a la probabilidad y a las consecuencias de un riesgo.

La estimación de riesgos puede abarcar costos, beneficios, preocupaciones de los interesados y otras variables, según convenga a la evaluación de riesgos.

3.6 Evaluación de riesgos: Proceso que consiste en comparar el riesgo calculado con ciertos criterios de riesgos para determinar la importancia del riesgo.

La evaluación de riesgos puede utilizarse para ayudar a tomar la decisión de aceptar o tratar un riesgo.

4 Términos Relacionados Con El Tratamiento Y Control De Riesgos

4.1 Tratamiento de riesgos: Proceso de selección y puesta en aplicación de medidas para modificar el riesgo.

El término "tratamiento de riesgos" se utiliza a veces para las propias medidas.

Las medidas de tratamiento de riesgos pueden incluir evitar, optimizar, transferir o retener el riesgo.

4.2 Control de riesgos: Acciones que ponen en aplicación las decisiones de la gestión de riesgos.

El control de riesgos puede incluir la supervisión, la reevaluación y la conformidad con las decisiones.

4.3 Optimización de riesgos: Proceso relacionado con el riesgo para minimizar las consecuencias negativas y maximizar las positivas y sus respectivas probabilidades.

En el contexto de seguridad, la optimización de riesgos se centra en la reducción del riesgo.

4.4 Reducción de riesgos: Acciones tomadas para reducir la probabilidad, las consecuencias negativas, o ambas, en relación con un riesgo.

4.5 Mitigación: Limitación de cualquier consecuencia negativa de un suceso particular.

4.6 Elusión de riesgos: Decisión de no involucrarse en una situación de riesgo o acción consistente en salir de la misma. La decisión debe ser tomada basándose en el resultado de la evaluación de riesgos.

4.7 Transferencia de riesgos: Puesta en común con otra parte de la carga de las pérdidas o el beneficio de las ganancias consecuencia de un riesgo.

Los requisitos legales o estatutarios pueden limitar, prohibir u ordenar la transferencia de cierto riesgo.

La transferencia de riesgos se puede llevar a cabo a través de un seguro o por otros medios.

La transferencia de riesgos puede crear nuevos riesgos o modificar un riesgo ya existente.

4.8 Financiación de riesgos: Provisión de los fondos necesarios para sufragar los costos del tratamiento de riesgos y los costos afines.

En algunas industrias, la financiación de riesgos se refiere sólo a la financiación de las consecuencias financieras relacionadas con el riesgo.

4.9 Retención de riesgos: Aceptación de la carga de las pérdidas o el beneficio de las ganancias consecuencia de un riesgo particular.

La retención de riesgos incluye la aceptación de riesgos que no se han identificado.

La retención de riesgos no recoge tratamientos que incluyan seguros o transferencia por otros medios.

4.10 Aceptación de riesgos: Decisión de aceptar un riesgo.

El verbo "aceptar" se ha elegido para transmitir la idea de que la aceptación tiene el significado básico que consta en el diccionario.

La aceptación de riesgos depende de los criterios de riesgos.

4.11 Riesgo residual: Riesgo que permanece después del tratamiento de riesgos.

ANEXO 2: Otras definiciones enfocadas a TI/SI[3]

1. **Activo:** Es un objeto o recurso de valor empleado en una empresa u organización
2. **Amenaza:** Es un evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.
3. **Vulnerabilidad:** Es una debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo.
4. **Riesgo:** Es la probabilidad de ocurrencia de un evento que puede ocasionar un daño potencial a servicios, recursos o sistemas de una empresa.
5. **Análisis:** Examinar o descomponer un todo detallando cada uno de los elementos que lo forman a fin de terminar la relación entre sus principios y elementos.
6. **Control:** Es un mecanismo de seguridad de prevención y corrección empleado para disminuir las vulnerabilidades.
7. **Evitar el riesgo:** El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades.
8. **Reducir el riesgo:** Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación controles y su monitoreo constante.

9. **Retener, Asumir o Aceptar el riesgo:** Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente.

10. **Riesgo Total:** La fórmula para determinar el riesgo total es: RT (Riesgo Total) = Probabilidad x Impacto Promedio A partir de esta fórmula determinaremos su tratamiento y después de aplicar los controles podremos obtener el Riesgo Residual